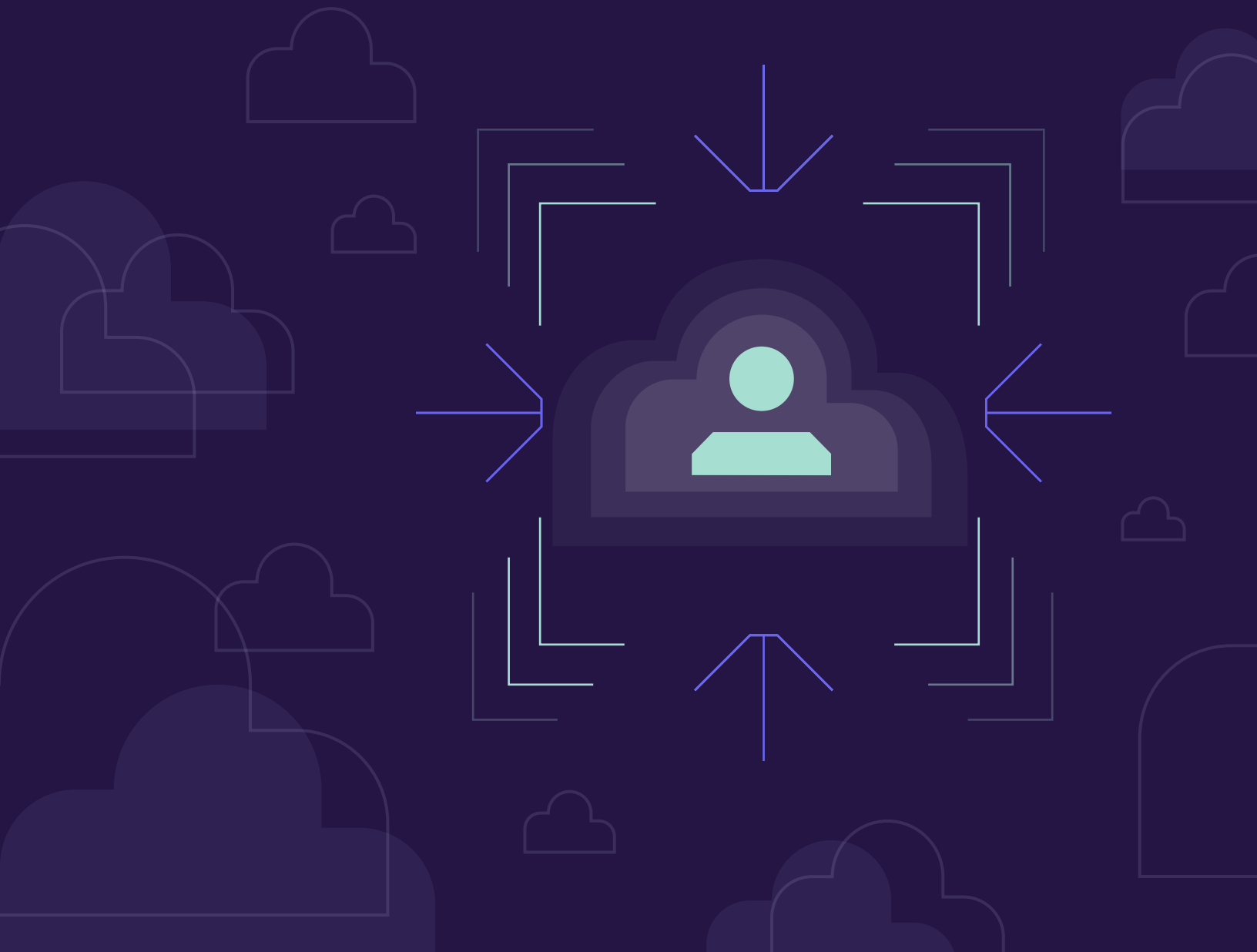
Abnormal

RESEARCH REPORT

2024 State of Cloud Account Takeover Attacks

A Call for Unified Visibility and Control



Executive Summary

83%
of respondents report their organization experienced an account takeover attack in the last year.

77%
of security leaders view account takeovers as a major threat.

99%
of security stakeholders cite account compromise prevention as a top priority.

63%
of survey participants are skeptical about MFA's effectiveness against these attacks.

99%
of respondents believe implementing a solution for detecting and automatically remediating compromised accounts in cloud services would greatly improve their defenses.

Already a severe threat, account takeover attacks, or ATOs, have grown in prevalence in recent years. Threat actors are making more attempts to harvest credentials, steal active session cookies, or otherwise gain access to email and cloud software accounts. Unfortunately, an escalation in attempted attacks creates additional opportunities for success—and more dire consequences.

There may be several reasons for this growth, including an uptick in phishing and social engineering—often integral elements of ATO attacks—fueled by the rise of generative AI. The widespread adoption of this new technology makes it easier than ever before to quickly generate greater volumes of more convincing attacks. As a result, threat actors can not only target a larger audience, but also use hyper-personalized messages customized for each recipient, greatly improving their chances of tricking end users.

Our latest Email Threat Report, for instance, shows that successful business email compromise attacks increased 108% year over year between 2022 and 2023, and phishing attacks remain the most prevalent threat—making up nearly three-quarters of all attacks received by Abnormal customers. The results can be devastating, with breaches involving stolen credentials costing an average of $4.62 million and taking 11 months to resolve.

While organizations are implementing measures to block account takeover attacks and more quickly detect when an account has become compromised, it will likely never be possible to entirely prevent account takeovers across every single application. Social engineering relies on human error, and tired, distracted, or careless employees will always make mistakes that enable threat actors to steal credentials that can either be used immediately or sold on the dark web. Further, brute force and credential stuffing attacks cannot be foiled 100% of the time.

For many security stakeholders, the phrase "account takeover" brings email account compromise to mind. But today's cloud application ecosystems are increasingly broad, interdependent, and complex. As these apps proliferate—and become ever more integral to key operational processes—additional points of entry into enterprise environments emerge. At the same time, it's progressively more difficult to maintain centralized visibility and unified control across diverse collections of cloud services. This is especially true when different business units are individually responsible for their own apps.

To better understand the challenges that security stakeholders face in this area, as well as how they are thinking about solutions, we surveyed over 300 security professionals across an array of global industries and organization sizes. Participants held leadership and practitioner roles, with more than one-third (34%) serving as the CIO, CISO, or VP of Security within their organization. Most (70%) were at a director, manager, or team lead level of seniority or above. Their organizations ranged in size from 1,000 employees to more than 25,000 employees.

In the report that follows, we'll explore the views of security stakeholders about the account takeover threat, what countermeasures they believe are needed, and what defenses today's vendors offer.

Table of Contents

Account Takeovers: A Grave and Growing Threat 4

Concerns About Account Takeovers 8

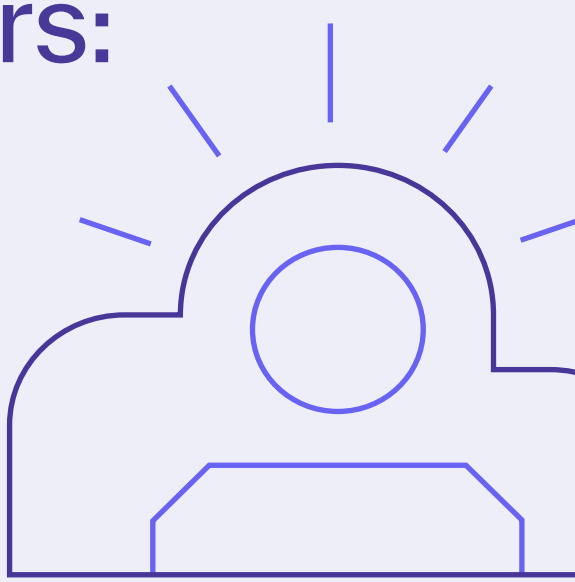
Defending Against Account Takeovers 14

Fighting Back Against Account Takeovers 22

Conclusion 27

About Abnormal 28

Account Takeovers: A Grave and Growing Threat



Not only are account takeover attacks among the favorite tactics of cybercriminals, but they also appear to be increasing in volume and frequency. Why? Because the compromise of an account can give attackers immediate access to company or customer data, enable embezzlement of funds, make it possible to launch additional attacks, or allow lateral movement across additional applications and connected platforms.

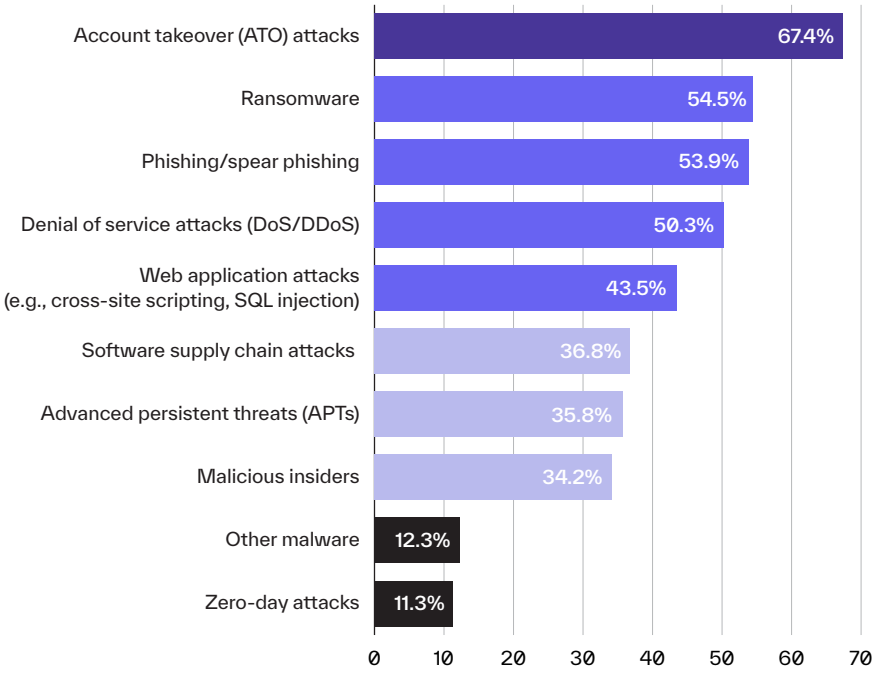
Research indicates that these attempts are occurring with accelerating frequency, with one study showing a 427% increase in attempts over the course of 2023. Most of these attacks target consumers, but they also contribute to billions in fraud losses for businesses of all sizes.

Account Takeovers Are a Leading Cybersecurity Concern

Given the increased volume of account takeover attacks—and the power that success puts into criminal hands—it's no surprise that two-thirds of survey participants (67.4%) listed account takeover attacks as one of the top four cyber threats that concerned them the most. This makes ATO attacks the leading worry for security leaders—even ahead of the threats that dominate headlines, like ransomware and spear phishing.

This worry is both logical and justified. After all, account takeover can result in immediate data loss, or it can serve as an enabling mechanism that allows attackers to gain persistent access to your environment. Once they've established this persistence, they're ready to plan, prepare, and launch other types of attacks, including ransomware.

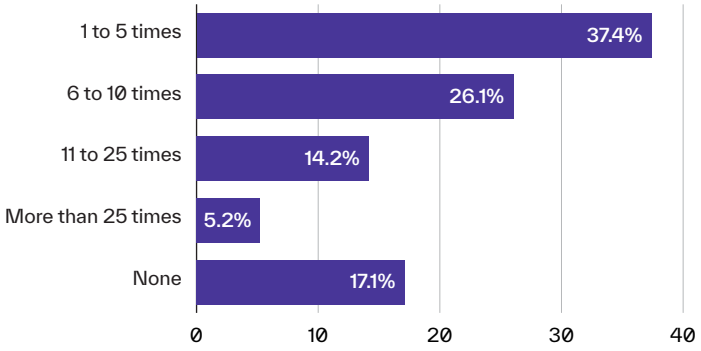
Which types of threats are the greatest concern for your organization? Select four.



The concern about account takeovers is certainly justified, as survey respondents are already experiencing this problem firsthand. A significant majority (83%) reported that their organization had been impacted by an account takeover attack at least once over the past year. Nearly half

of organizations (45.5%) were impacted by ATO attacks more than five times over the past year, while almost 20% had experienced more than 10 significant ATO attacks.

Which option best describes the number of times your organization has been impacted by an account takeover attack (across all applications) in the past year?



The consequences of an account takeover attack can be extensive and include significant breach-associated financial losses, business disruption, and reputational damage. While we didn't ask respondents to specify the exact impact of the attacks they experienced, we can assume that these attacks were successful to some degree.

However, what we cannot assume is that the 17% of survey participants who did not report impactful ATO attacks are in the clear. Because account compromise is often associated with long attacker dwell times, it may well be the case that some of these organizations have compromised accounts within their environments that simply have not yet been detected.

How Compromised Accounts Contributed to Well-Known Breaches:

- **Colonial Pipeline:** A single compromised password reportedly resulted in this ransomware attack, which led to the shutdown of the largest fuel pipeline in the United States and gasoline shortages along the East Coast. Subsequent investigation revealed that the attackers gained access to the corporate network through an inactive virtual private network (VPN) account. The login credentials belonging to the employee who owned the account appear to have been reused from another website that was previously compromised.
- **Electronic Arts:** The breach that resulted in the game publishing company's loss of a treasure trove of valuable intellectual property, including source code for *FIFA 21*, began when the attackers used stolen session cookies to gain access to an internal Slack channel. Once inside Slack, the attackers messaged IT support, asking for a multifactor authentication token that they claimed they needed due to a lost mobile device. With this token, they were able to log onto a virtual machine, explore the corporate network, and then download data and source code.
- **Uber:** The ride-sharing and transportation giant disclosed that its internal networks had been breached after an attacker reportedly compromised an employee's Slack account and then moved laterally between systems, eventually finding highly privileged credentials on a network file share. In what's been described as a "complete compromise," the attacker was then able to access customer data, the company's public cloud infrastructure and production systems, and the management portal for its endpoint detection and response (EDR) software.
- **U.S. Government:** Thought to have been executed by nation-state-level attackers based in China, this attack targeted officials in the U.S. State Department and Department of Commerce, as well as government agencies in Western Europe. The threat actors exploited a vulnerability in the Microsoft Exchange authentication process, which enabled them to access email accounts from which they could view and steal sensitive data.

Concerns About Account Takeovers

Because compromised accounts give cybercriminals far-reaching and often long-lasting access to corporate resources, these attacks are notoriously expensive and difficult to remediate. According to research from IBM, it takes an average of 11 months to resolve a breach caused by stolen credentials—240 days to detect the breach and another 88 days to contain and resolve it. Plus, a breach resulting from credential theft costs its victim an average of $4.62 million.

Further, credential compromise was the most common entry point in the breaches analyzed in the Verizon 2024 Data Breach Investigations Report, with attackers using this method nearly twice as often as the next most common tactics—phishing and vulnerability exploits.

Knowing this, we asked security leaders about their most pressing concerns regarding how and where account takeovers happen.

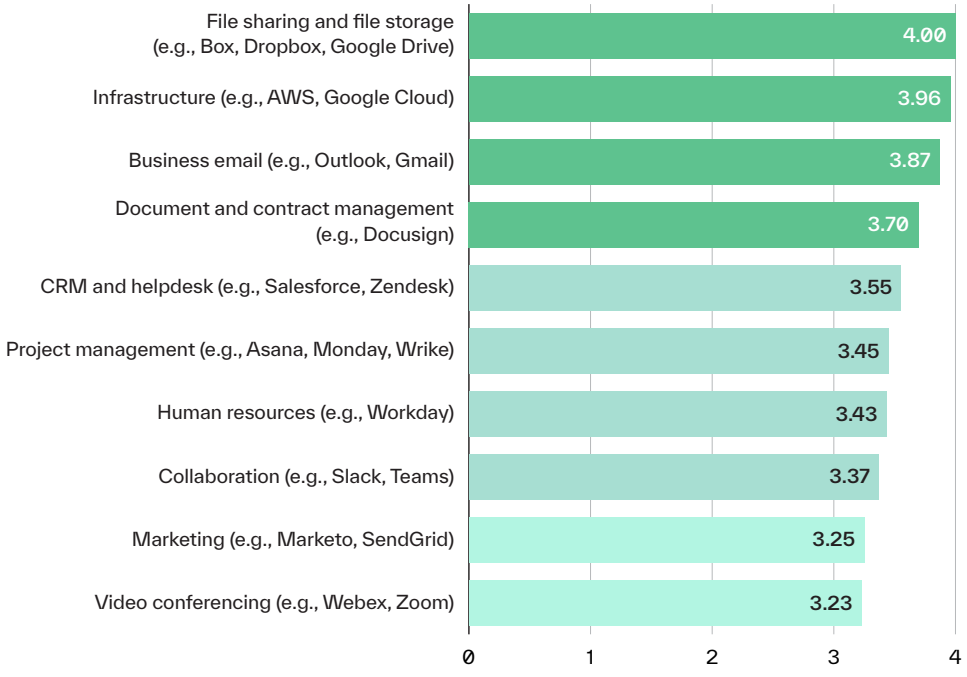
Concern by Type of App Being Targeted

We first asked survey participants about the cloud services their organizations rely on. Which ones, if compromised, would allow an attacker to cause the most harm?

Their top-ranked responses were file storage and sharing services, such as Dropbox and Box, and cloud infrastructure services, which include Amazon Web Services, Microsoft Azure, and Google Cloud Platform. This makes sense, as file storage and sharing services enable immediate access to (and exfiltration of) organizational data—including sensitive, regulated, or proprietary data. And the compromise of cloud infrastructure allows for wide-ranging lateral movement across the environment, with potential impacts on customer-facing and revenue-generating services, as well as those embedded in critical operational processes.

Also near the top were business email accounts, such as Microsoft Outlook and Gmail, and document and contract management software like Docusign. These, too, represent significant risks. Email account compromise can give attackers access to a treasure trove of data, and the ability to launch further attacks on employees and customers. Meanwhile, compromising document or contract management systems can result in financial losses, theft of sensitive information, or legal repercussions.

On a scale of 1 (not at all) to 5 (extremely), rate your concern for an account takeover attack against each of the following types of cloud-delivered business tools and services:



Even the tools and services that respondents were less concerned about are still important, as their compromise could potentially have major consequences.

For instance, while Slack landed near the bottom of the list, it is used for internal communications by more than 100,000 organizations, including nearly 80% of Fortune 100 companies. This makes it an attractive target for threat actors. Recent research from Enterprise Strategy Group indicates that 89% of organizations have experienced an attack on collaboration tools, and 52% have been targeted in a multi-channel attack coordinated across email and a connected app like Slack.

The compromise of popular enterprise software solutions like Workday and Salesforce can have even farther-reaching impacts. Gaining access to Workday, for instance, can enable threat actors to view bank account information and other personal data, leaving employees vulnerable to identity theft.

SaaS Account Compromise Facilitates Lateral Movement in Recent Breaches

- **AWS + Cloud Infrastructure:** After operating a sophisticated credential-stealing campaign targeting AWS environments, TeamTNT expanded its operations in mid-2023 to target Microsoft Azure and Google Cloud Platform, focusing on the exploitation of misconfigurations and unpatched vulnerabilities. Recent news suggests that TeamTNT is developing what's been described as an "aggressive cloud worm" designed to harvest credentials and facilitate resource hijacking.
- **Atlassian:** A suspected nation-state attacker reportedly compromised an internal Atlassian server belonging to Cloudflare. After gaining access to the self-hosted server, the threat actors were able to access the company's Confluence and Jira systems, as well as a source code management platform that used Atlassian Bitbucket. Initial access was obtained through the use of tokens and service account credentials stolen during a previous compromise linked to the October 2023 Okta breach.
- **Zendesk:** The customer support software provider informed customers that it had suffered a data breach after multiple employees were tricked into revealing account credentials to attackers during a sophisticated SMS phishing campaign. With these credentials, the attackers were able to access log data that may have belonged to customers.

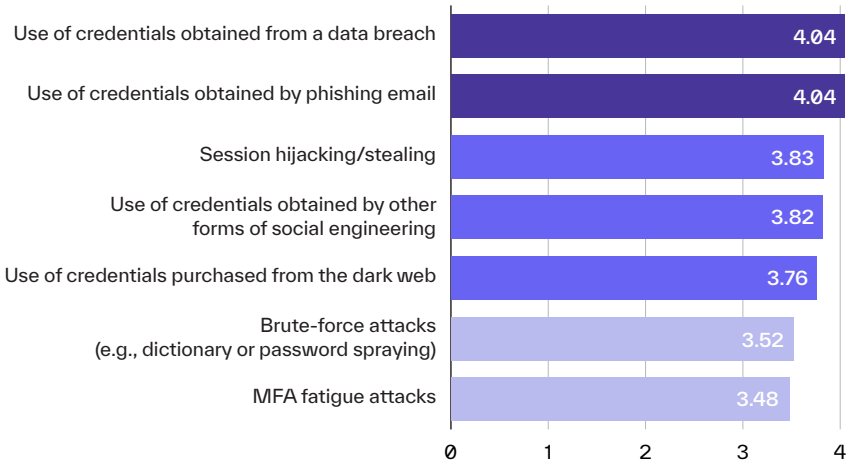
Concern by Type of Tactic Being Used

Next, we asked survey participants which specific ATO attack *tactics* concerned them the most.

Tied for first place were the use of credentials obtained through a data breach and the use of credentials obtained through phishing. It's likely that these responses were top-ranked because they are the attack tactics that security stakeholders see most often. After all, social engineering (which includes phishing) was involved in 45% of all breaches analyzed in the 2024 Verizon Data Breach Investigations Report. The number of business email compromise (BEC) attacks observed by Abnormal Security also increased by 108% between 2022 and 2023.

This growth may well be driven by attackers' use of generative AI to create more authentic-looking phishing messages faster. Credentials continue to be harvested at scale in major breaches around the world—often before the breach victims even realize that an incident has taken place.

On a scale of 1 (not at all) to 5 (extremely), rate your concern for each approach that can be used to perpetrate an account takeover attack:



Session hijacking was also highly ranked. With more and more session cookies now available for sale on the dark web, it's easier than ever for an attacker to gain access to an active login session—especially on a collaboration app like Slack, where it's then possible to circumvent multi-factor authentication (MFA) protections to gain persistent or repeat access.

Lower ranked in our survey (but still high risk) is the use of credentials obtained through other forms of social engineering. Depending on the type of attack and their "freshness," these credentials may be just as immediately useful as those acquired through phishing. Conversely, credentials purchased on an underground forum are more likely to be expired or invalid since their buyers have less control over or visibility into how and when they were obtained.

Even the ATO tactics deemed by security leaders to be less pressing concerns remain a considerable threat. For example, brute force attacks can be mitigated if end users consistently employ strong passwords and system administrators impose limits on the number of guesses a user can make before authentication is locked, but it is nearly impossible to eliminate these risks completely.

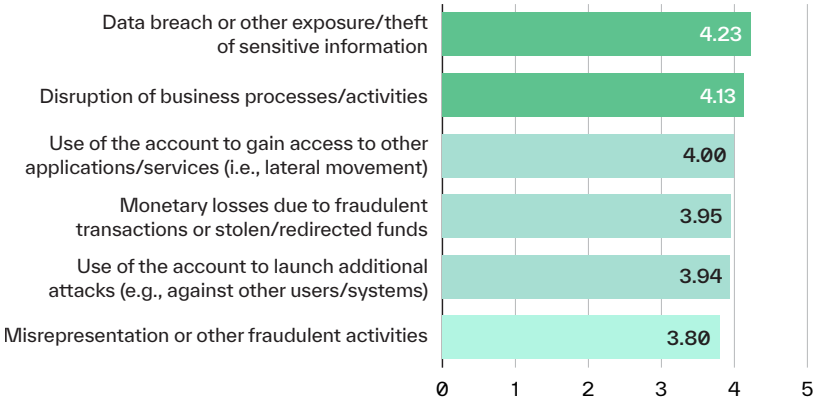
MFA fatigue attacks, in which attackers send a barrage of push notifications to a legitimate user's device in an effort to frustrate or distract the user into accepting the request to stop the notifications, rely on human error, and are thus difficult to defend against. In recent years, MFA fatigue attacks have been used to successfully compromise accounts at both Microsoft and Cisco.

Concern by Potential Impact of the Attack

We also asked stakeholders about the potential impacts of an ATO attack and which damages were most concerning to them.

Survey participants cited data breaches, along with the exposure or theft of sensitive information, as their top concern. Disruption of business processes followed close behind, and the next three responses were tightly clustered, indicating fairly similar levels of concern.

On a scale of 1 (not at all) to 5 (extremely), rate your concern for the following potential impacts of an account takeover attack:



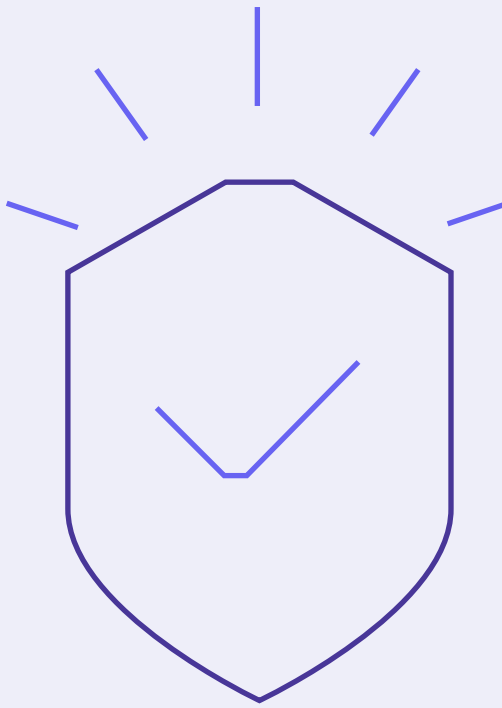
Data exfiltration or compromise is typically the end goal of attackers, so it makes sense that stakeholders are most worried about attacks that immediately result in what is often a late-stage attack objective. When an account with access to regulated or sensitive information is compromised, the event typically must be considered (and treated) as a breach, even if there's no evidence that data was exfiltrated at scale. Further, disruptions to the business can have immediate financial repercussions due to loss of revenue or compromise of customer experience.

The following three impacts were also of significant concern:

- Use of the compromised account to gain access to other resources
- Monetary losses due to fraudulent transactions
- Use of the account to launch additional attacks

However, these activities represent only intermediate attack stages or a single portion of the financial fallout that a major data breach can cause. Therefore, they are (appropriately) not at the very top of the list of concerns.

Defending Against Account Takeovers



Part of the reason account takeover attacks are a rising threat is because the preventative measures currently in place to mitigate this risk are only partially effective. The prevailing strategies include implementing fraud detection mechanisms, requiring multi-factor authentication, and encouraging strong password use. To be sure, all of these measures *can decrease* the risk of account compromise, but none can eliminate it entirely. Unfortunately, it remains challenging to detect an attack in time to prevent far-reaching damage—especially since a data breach often follows immediately from the attack.

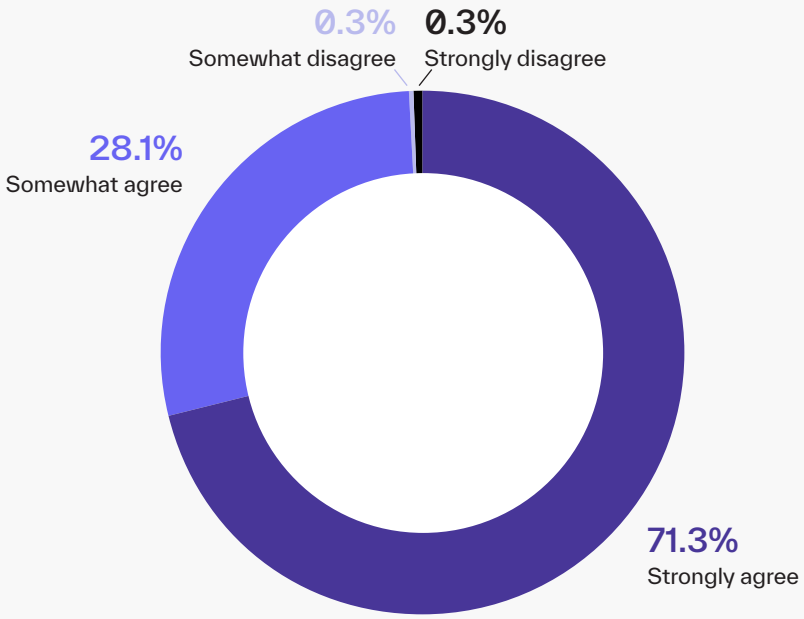
Prevention Is a Top Concern

Since account takeover attacks can have large-scale consequences for customer privacy, compliance, data security, brand reputation, and operational integrity, security leaders are understandably invested in preventing them.

When asked about their concern levels, nearly all of the security stakeholders we surveyed agreed that preventing compromised accounts was among their top security priorities. Nearly three-fourths of respondents strongly agree that preventing account takeovers is a top concern, while the remaining one-fourth stated that they somewhat agreed with that sentiment.

Knowing that they are worried about effectively preventing account takeovers, we next asked survey participants to evaluate the effectiveness of several commonly employed protection mechanisms.

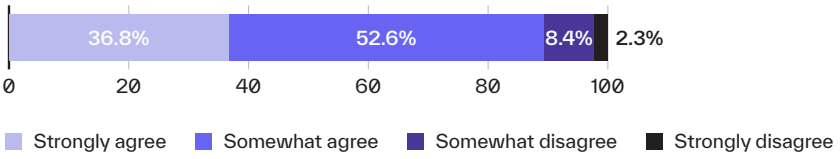
Describe your agreement with the following statement:
"Preventing account takeover attacks —especially those targeting enterprise-wide cloud applications or services — is a top security concern for my organization."



The Efficacy of Multi-Factor Authentication

Recommended by NIST and Microsoft, MFA has been viewed as an industry-wide gold standard in ATO prevention. Nonetheless, a mere 37% of respondents have strong confidence in its effectiveness in protecting against these attacks.

"We use MFA or passkeys for all/most accounts,and this gives us confidence that we are protected against ATO attacks."



Bad actors have been finding more ways to bypass MFA more often—making MFA less effective at preventing account compromise. For example, a number of threat groups, including Robin Banks and EvilProxy, are now offering MFA bypass as-a-service kits for sale. Using stolen MFA tokens, the kits make it possible to hijack active authentication sessions, lowering the barrier to entry for amateur threat actors, who simply need to purchase one of these kits to begin circumventing MFA. This tactic is a favorite of extortion-only ransomware affiliate Lapsus$, which names Microsoft, Okta, and Nvidia among its victims. The bypass of MFA also played a prominent role in the high-profile and widely damaging SolarWinds attack.

Threat researchers have observed a significant increase in MFA bypass attacks over the past year. An investigation conducted by Kroll Advisory discovered that 90% of the successful adversary-in-the-middle (AiTM) and business email compromise (BEC) attacks it analyzed occurred while MFA was already in place.

These threats aren't going unnoticed, which is likely why only 37% of security leaders see MFA as an effective way to prevent attacks. Among security stakeholders, there's increasing awareness that while newer authentication methods offer more robust protection, MFA is not a fail-safe.

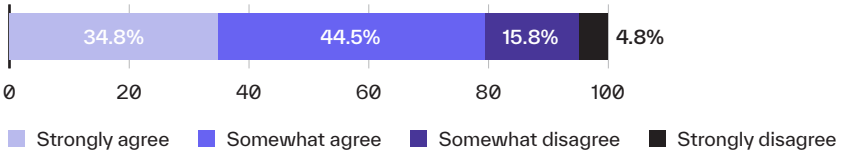
The Efficacy of SSO and Native Security Technologies

Survey participants are even less confident in single sign-on (SSO) technology, another widely implemented ATO protection measure with limited efficacy. A full 65% of respondents lacked confidence in SSO's ability to protect against compromised accounts.

SSO does have benefits—for instance, making security monitoring easier by serving as a single source of log data and events. With SSO in place, it's easier to apply rules requiring strong passwords since these have to be enforced in only one place, rather than across multiple cloud apps and services. It's also easier to enforce MFA when SSO is implemented.

However, SSO still has a significant downside: once compromised, it offers attackers ease and simplicity when it comes to lateral movement across the environment.

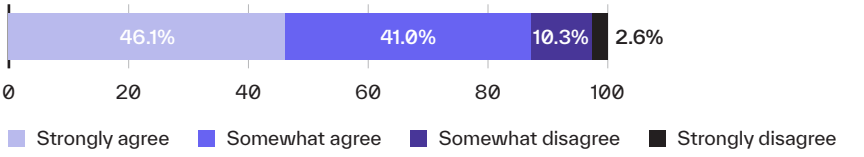
"We use single sign-on (SSO) for all/most accounts, and this gives us confidence that we are protected against ATO attacks."



In addition, many survey participants report that they rely on each individual cloud software vendor to supply native protections against account take-over attacks. Nearly half of respondents strongly agreed that this was something they expected of their cloud services, while 87% generally agreed.

In many cases, this may not match the reality of what cloud software vendors actually offer or are able to achieve. After all, Salesforce, Workday—and the providers of all the other applications we mentioned in the survey—aren't security companies. Most apps do offer security features, but these tend to be safeguards against misconfiguration or allocating too many privileges to too many users, rather than real-time guardrails against account takeover.

"We expect each cloud application/service to provide security features to protect us from ATO attacks."

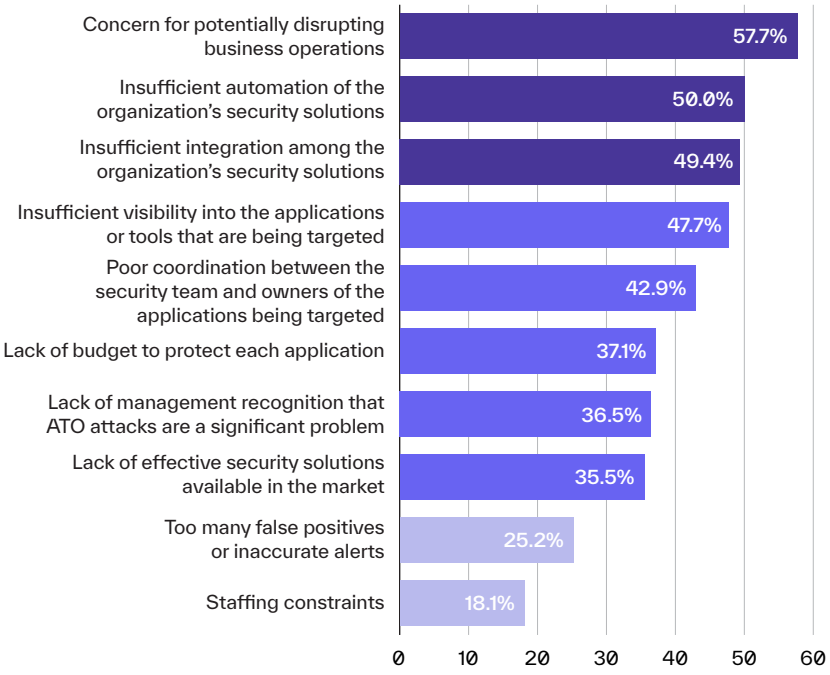


Many SaaS providers assume that their products will be used in conjunction with an identity and access management (IAM) or identity governance and administration (IGA) platform that will provide an effective layer of protection. Others may assume that customers will rely on MFA implemented outside of the app, which, as we've already discussed, is not fail-safe.

Top Obstacles to Defending Against Account Takeovers

Given the large number of successful account takeovers and their devastating consequences, it's clear that defenses—across geographies, organizational sizes, and industries—could be more effective than they are today. To better understand why this is a growing problem, we asked survey participants about their top obstacles to preventing account takeovers.

Which of the following factors most inhibit your organization's ability to defend against account takeover attacks? Select four.



The top response was concern about potential business disruptions, chosen by nearly 60% of survey participants. This is understandable, as automatically blocking account access when suspected ATO activity is detected can drastically interfere with operations—especially when this access is for mission-critical business applications.

Insufficient automation, also near the top of the list of inhibitors, was mentioned by half of the participants. Again, this is reasonable, given the need for speed in effective defense. Insufficient integration among the organization's security solutions was similarly ranked. This response is closely related to the next-most highly ranked inhibitor: insufficient visibility. To counter these threats, security teams need consistent, uniform visibility and control across often disparate ecosystems of cloud

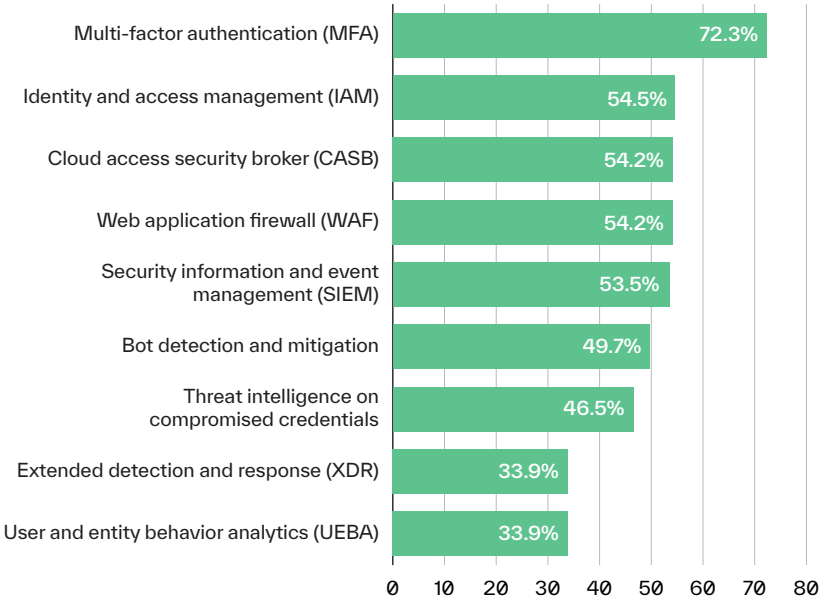
apps and services. Unfortunately, it's common for currently available tools to offer only fragmented visibility, protect only some applications, and neither correlate events nor deliver actionable insights.

In addition, more than 40% of survey participants mentioned inadequate collaboration between application owners and security teams among their top barriers to successful defense. For instance, it's typical for the HR department to own Workday while the sales department manages Salesforce. When these sorts of silos exist, security teams lack administrative responsibility and visibility into these key business applications—making them much harder to protect.

Current and Future Countermeasures Against ATO

To gain a better understanding of how today's organizations defend against account takeovers, participants were asked about their current strategies and future plans. Despite misgivings about its effectiveness, organizations continue to invest in MFA, likely because it is well known, vendors have name recognition, and its use is thought of as a best practice. In fact, a full 72% of survey participants either have already implemented MFA or plan to do so within the next 12 months. This is the case despite the fact that 63% do not have strong confidence in MFA's ability to protect against account takeover attacks.

Which countermeasures does your organization currently use or plan to use (within 12 months) to help defend against account takeover attacks? Select all that apply.



Other frequently mentioned solutions included identity and access management (IAM), cloud access security brokers (CASB), and web application firewalls (WAF), which were all cited by more than 50% of respondents. But these solutions weren't explicitly designed to counter the account takeover threat. While useful for protecting web applications from malicious traffic, WAFs have few capabilities that can be applied to guard against account takeovers. Further, CASB solutions, once imagined to offer unified visibility across cloud application ecosystems, have fallen far short when it comes to defending against the account takeover threat. And, unfortunately, IAM solutions simply cannot guard against sophisticated social engineering or session hijacking tactics.

It's interesting to note that user and entity behavior analytics (UEBA) is at the bottom of the list of countermeasures, though more than one-third of survey participants (33.9%) *do* have plans to implement this technology. While behavioral analysis is exactly what's needed to detect malicious activity within cloud apps, the fact that it is at the bottom of the list may be because first-generation UEBA tools didn't deliver the hoped-for results. Because they weren't leveraging AI—and because analytics weren't yet mature—detection accuracy was lacking. UEBA might also be low-ranked because next-generation solutions are fairly new to the market, and awareness remains limited.

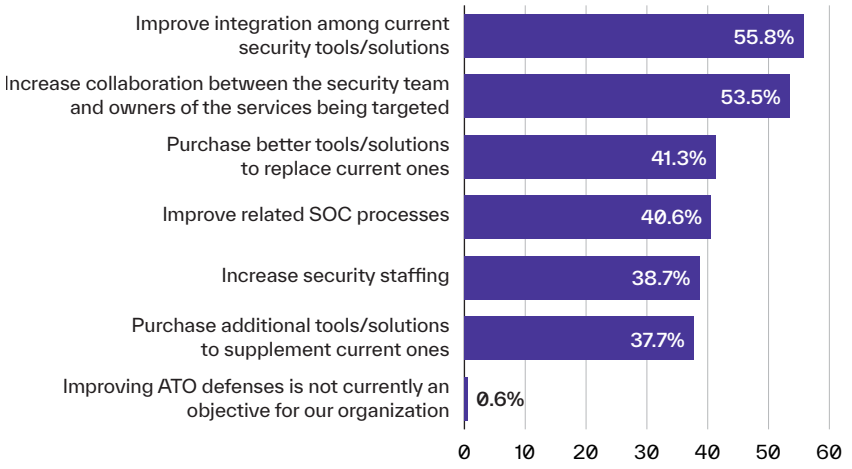
Fighting Back Against Account Takeovers

It's clear that account takeovers remain an issue at least partially because organizations are implementing and relying on solutions like MFA and SSO—despite a lack of confidence in their abilities *and* the fact that these tools were not designed to stop in-progress attacks. So what *is* needed to effectively defend against account takeovers?

Necessary Improvements to Today's Tools

We first asked survey participants about their top priorities for improving their ability to defend against account takeover attacks within the next year. Highest on the list of wished-for improvements was better integration among current security tools and solutions. Such integration is key because these attacks typically leave multiple signals across different applications—particularly as threat actors move between platforms.

What are your organization's top priorities over the next 12 months for improving its defenses against account takeover attacks? Select up to three.



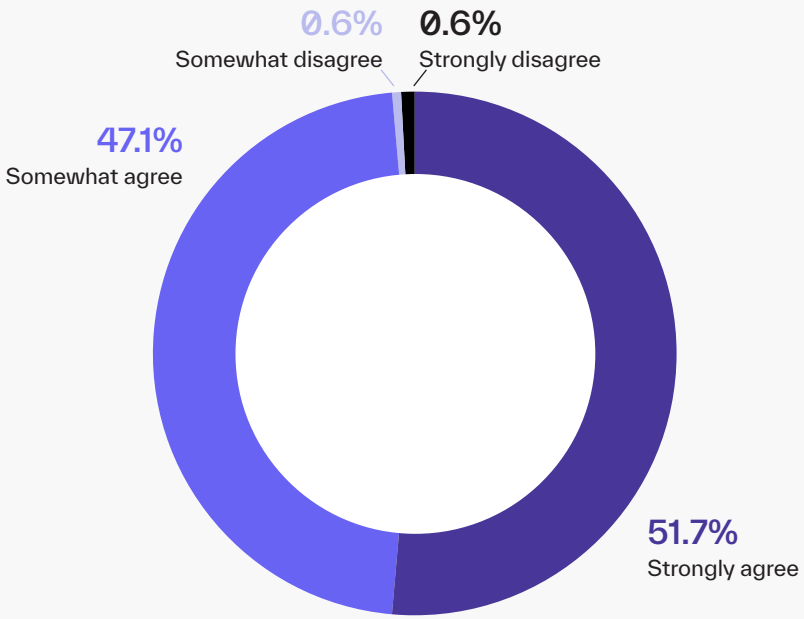
Also highly ranked was improving collaboration between security teams and application owners. This is especially important to executive leaders, 62% of whom cited it as a priority. The lesson is clear: silos—whether organizational, operational, or relating to data and visibility—impede security teams' ability to detect and block these attacks, ultimately hurting the organization as a whole.

Additionally, over one-third of participants mentioned the need to replace current tools and solutions with better ones. This is likely a result of the dissatisfaction leaders feel with the capabilities that are most widely available and most popular today—underscoring the need for a new and radically better approach.

Top Characteristics in the Ideal Solution

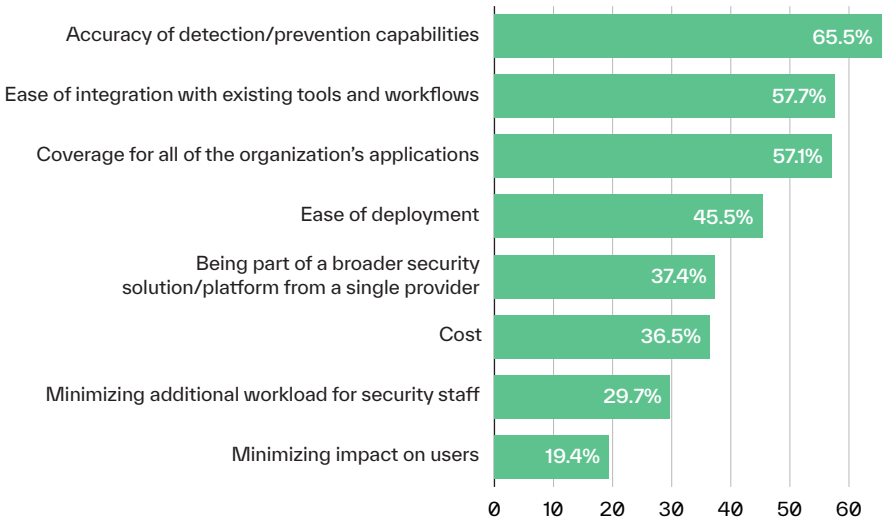
When we asked security leaders about their needs, one thing was nearly unanimous: they desire a tool that not only identifies account takeovers but will also automatically remediate them.

Describe your agreement with the following statement:
"My organization's defenses against ATO attacks would be significantly enhanced by a solution that can accurately detect compromised accounts across our various cloud applications and services and automatically remediate them."



To understand what other features may be needed, we also asked survey participants what the characteristics of an ideal solution would be.

Which are the most important capabilities/characteristics of an ideal solution for defending against account takeover attacks? Select up to four.



Detection accuracy was the most important aspect, cited by two-thirds of all respondents as a top-four characteristic. This was closely followed by the ease of integration with existing tools and workflows (58%), coverage for all of the organization's applications (57%), and ease of deployment (46%).

Accuracy and coverage for all of the organization's apps were particularly important to executive leaders, while hands-on practitioners listed accuracy and ease of integration as their top characteristics.

An Abnormal Approach to Unifying Account Takeover Protection

With the lack of cross-platform visibility and few ways to control the full spectrum of enterprise applications, it's clear that there is a need for a new approach to account takeover detection and remediation. To help organizations protect themselves from this threat, Abnormal has created a next-generation solution built to meet the needs of security leaders that features the following elements:

Behavioral AI Approach

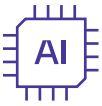
Using a fundamentally different approach from legacy systems, the solution leverages user and entity behavior analytics to profile and baseline good behavior via AI. It performs identity modeling to understand typical behavior for each individual across every platform, enabling the solution to detect anomalous activity no matter where it occurs.

API Architecture and Integrations

The solution connects to enterprise applications via an API to harvest the signals and data needed to understand user behavior. These include unusual geolocations, dangerous IP addresses, changes in mail filter rules, unusual device logins, privilege escalations, and more. Because it can connect to applications within collaboration platforms, cloud infrastructure, and other areas, the solution can detect attacks everywhere.

Unified Profiles with Notable Events

The solution correlates all data in an easily-accessible database so that security teams can identify when an account takeover has occurred and take action. This gives analysts immediate access to every piece of relevant information across all notable events in one place and visibility into the full attack chain. This way, they can quickly determine the best way to remediate the attack.



AI-Powered Auto-Remediation

By leveraging user and entity behavior analytics to automatically determine that enough malicious activity has taken place to signal compromise, the solution can act *with high confidence*. It can then auto-remediate accounts, kicking hijackers out of all compromised platforms before any further damage can be done.

A truly integrated solution offering complete visibility across the entire cloud ecosystem, protecting all applications, correlating events to enable contextual awareness, generating actionable insights, and automating remediation wasn't available in the past.

Abnormal's unified Account Takeover Protection provides all of these capabilities—effectively preventing account takeover attacks and remediating account compromise for security teams worldwide.

Conclusion

The threat posed by account takeover attacks has long been pressing and severe, but recent technological advances have made it easier than ever for cybercriminals to trick end users into giving up their credentials. Threat actors today use an array of effective strategies—ranging from brute forcing and credential stuffing to session hijacking—to gain access to business email and cloud software accounts.

Participants in our survey recognize that even a single instance of account compromise can be extremely damaging. Worries about this threat can keep security stakeholders up at night, and those who took part in our survey are far from exempt from these industry-wide concerns.

Not only can account takeover attacks be widely and almost instantly destructive, but the tools that security teams have relied on to detect and stop them aren't adequate for the problem at hand. Solutions like MFA, IAM, WAFs, and CASBs provide valuable protection, but they're not enough to completely mitigate the real-world risks that this threat poses. Such solutions may reduce the number of successful account takeover attempts but offer few ways to detect and automatically remediate compromised accounts. And because account takeover attacks unfold so quickly, *automatic* remediation is needed, given the speed advantage it offers.

Security professionals need an entirely new approach. This is what Abnormal has built, and we're now making it available through unified Account Takeover Protection—with coverage for all the applications that enterprises use most.

Abnormal

Abnormal Security is the leading AI-native human behavior security platform, leveraging machine learning to stop sophisticated inbound attacks and detect compromised accounts across email and connected applications. The anomaly detection engine leverages identity and context to understand human behavior and analyze the risk of every cloud email event—detecting and stopping sophisticated, socially-engineered attacks that target the human vulnerability.

You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly. Additional protection is available for Slack, Workday, Salesforce, ServiceNow, Zoom, Amazon Web Services and multiple other cloud applications.

Interested in Auto-Remediating Account Takeovers?

Protect your cloud applications with unified Account Takeover Protection.

Request a Demo → See the Product →